UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/029,088	10/19/2001	Gary Milo	2590/102	3440

2101 7590 02/18/2005

BROMBERG & SUNSTEIN LLP
125 SUMMER STREET
BOSTON, MA 02110-1618

EXAMINER	
LAZARO, DAVID R	
ART UNIT	**PAPER NUMBER**
2155	

DATE MAILED: 02/18/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/029,088	MILO, GARY	
	Examiner	Art Unit	
	David Lazaro	2155	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *19 October 2001*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-17* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-17* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *19 October 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *01/16/02, 02/26/03,* 3/23/04 -DRL
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-17 are pending in this Office Action.

Papers Received

2. Most recent Change of Address was received on 12/27/04.

3. The Petition to Accord Correspondence Filing Data Shown on Express Mail Label "Date-In" was received on 02/25/02.

Priority

4. This application claims the benefit of 60/313,577 (08/16/01).

Information Disclosure Statement

5. The information disclosure statements (IDS) submitted on 01/16/02, 02/26/03 and 03/23/04 have been considered by the examiner.

Claim Rejections - 35 USC § 112

6. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

7. Claim 10 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

8. Claim 10 recites the limitation "the hierarchical value ascribed to the source address associated with each packet" in lines 8-9 of the claim. There is insufficient antecedent basis for this limitation in the claim. The examiner notes that in lines 4-6, a "hierarchical value" was ascribed to "a subset of addresses on the external network". It is not distinctly clear if "the source address associated with each packet" is limited to the "subset of addresses on the external network".

Claim Rejections - 35 USC § 102

9. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

10. Claims 1-17 rejected under 35 U.S.C. 102(e) as being anticipated by U.S. Patent 6,519,703 by Joyce (Joyce).

11. With respect to Claim 1, Joyce teaches an interface between a site and an external network for screening packets on the external network, each packet having an associated source address (Col. 2 lines 30-40 and Col. 4 lines 48-54), the interface comprising: a. an heuristic profiler for ascribing a characteristic value (Col. 2 lines 41-65) to each address on the external network (Col. 4 lines 14-21 and lines 44-60) based at least on prior activity associated with the address (Col. 3 lines 29-67 and Col. 4 lines

44-60); and b. a filter for selectively passing a particular packet from the external network to the site based at least on the characterizing value ascribed by the heuristic profiler to the source address associated with the particular packet (Col. 2 lines 30-40 and Col. 3 lines 29-58).

12. With respect to Claim 2, Joyce teaches all the limitations of Claim 1 and further teaches wherein the heuristic profiler ascribes a characteristic value to each known address on the external network based at least on characteristics of prior packets received by the site bearing the source address associated with the particular packet (Col. 3 lines 29-67 and Col. 4 lines 44-60).

13. With respect to Claim 3, Joyce teaches all the limitations of Claim 1 and further teaches the site is a computer (Col. 3 lines 1-15 and Col. 7 lines 6-16).

14. With respect to Claim 4, Joyce teaches all the limitations of Claim 1 and further teaches the site is a local network of computers (Col. 3 lines 1-15 and Col. 7 lines 6-16).

15. With respect to Claim 5, Joyce teaches all the limitations of Claim 1 and further teaches the site is a web server (Col. 3 lines 1-15 and Col. 7 lines 6-16).

16. With respect to Claim 6, Joyce teaches all the limitations of Claim 1 and further teaches further comprising a firewall in communication with the site, the firewall interposed between the site and the network (Col. 2 lines 16-40 and Col. 3 lines 1-15).

17. With respect to Claim 7, Joyce teaches all the limitations of Claim 1 and further teaches a load monitor for monitoring the traffic of packets between the network and the site relative to a specified nominal load (Col. 3 lines 29-67 and Col. 4 lines 34-60).

18. With respect to Claim 8, Joyce teaches all the limitations of Claim 7 and further teaches filter selectively passes a particular packet based at least on the monitored traffic of packets (Col. 3 lines 29-67 and Col. 4 lines 34-60).

19. With respect to Claim 9, Joyce teaches all the limitations of Claim 1 and further teaches a history module for developing a time profile of observations of packets received from associated source addresses (Col. 3 lines 29-67 and Col. 4 lines 34-60).

20. With respect to Claim 10, Joyce teaches a method for screening a flow of packets between a site and an external network each packet having an associated source address (Col. 2 lines 30-40 and Col. 4 lines 48-54), the interface comprising: a. ascribing a hierarchical value (Col. 2 lines 41-65) to a subset of addresses on the external network (Col. 4 lines 14-21 and lines 44-60) based at least on prior activity associated with each address of the subset (Col. 3 lines 29-67 and Col. 4 lines 44-60); and b. selectively passing packets from the external network to the site based at least on the hierarchical value ascribed to the source address associated with each packet (Col. 2 lines 30-40 and Col. 3 lines 29-58).

21. With respect to Claim 11, Joyce teaches all the limitations of Claim 10 and further teaches checking each packet for compliance with specified protocol standards (Col. 3 lines 29-67 and Col. 4 lines 34-43).

22. With respect to Claim 12, Joyce teaches all the limitations of Claim 10 and further teaches developing a time profile of observations of packets received from associated source addresses (Col. 3 lines 29-67 and Col. 4 lines 34-60).

23. With respect to Claim 13, Joyce teaches all the limitations of Claim 10 and further teaches the step of monitoring the traffic of packets between the network and the site relative to a specified nominal load (Col. 3 lines 29-67 and Col. 4 lines 34-60).

24. With respect to Claim 14, Joyce teaches all the limitations of Claim 13 and further teaches the step of setting a threshold standard based on the monitored traffic of packets between the network and the site (Col. 3 lines 16-67 with particular note of lines 20-25 and lines 61-67, and Col. 4 lines 34-60).

25. With respect to Claim 15, Joyce teaches all the limitations of Claim 14 and further teaches wherein the step of selectively passing packets from the external network to the site is based, at least in part, on the hierarchical value ascribed to the source address associated with each packet relative to the threshold standard (Col. 3 lines 16-67).

26. With respect to Claim 16, Joyce teaches A method for characterizing a subset of a universe of network addresses, each address corresponding to an associated device, the method based at least on observation of a transmission from each associated device (Col. 2 lines 30-40 and Col. 4 lines 48-54), the method comprising: a. recording occurrence of an observation (Col. 4 lines 34-60); b. recording a time associated with the observation (Col. 4 lines 14-21 and lines 44-60); c. retaining a timed profile of observations of transmissions from each associated device; and d. using the timed profile to assign a hierarchical value to each network address of the subset (Col. 4 lines 44-60 and Col. 3 lines 29-59).

27. With respect to Claim 17, Joyce teaches a computer program product for use on a computer system for screening data flow between an external network device and a

local site (Col. 2 lines 30-40 and Col. 4 lines 48-54), the computer program product comprising a computer usable medium having computer readable program code thereon, the computer readable program code comprising: a. program code for ascribing a hierarchical value (Col. 2 lines 41-65) to a subset of addresses on the external network (Col. 4 lines 14-21 and lines 44-60) based at least on prior activity associated with each address of the subset (Col. 3 lines 29-67 and Col. 4 lines 44-60); and program code for selectively passing packets from the external network to the local site based at least on the hierarchical value ascribed to the source address associated with each packet (Col. 2 lines 30-40 and Col. 3 lines 29-58).

Conclusion

28. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

29. U.S. Patent 6,321,338 by Porras et al. "Network Surveillance" November 20, 2001. Discloses profiling of network addresses and detection of suspicious activity through comparison of a short term profile to a long term profile. Does not explicitly disclose filtering packets based on detection.

30. U.S. Patent Application Publication 2002/0107960 by Wetherall et al. "Network Traffic Regulation Including Consistency Based Detection and Filtering of Packets with Spoof Source Addresses" August 8, 2002. Discloses statistical comparisons for filtering purposes based on consistency measures related to network addresses.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to David Lazaro whose telephone number is 571-272-3986. The examiner can normally be reached on 8:30-5:00 M-F.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Hosain Alam can be reached on 571-272-3978. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

David Lazaro
February 15, 2005

HOSAIN ALAM
SUPERVISORY PATENT EXAMINER